EL548970229US

METHOD AND APPARATUS FOR PROTECTION SWITCHING IN VIRTUAL PRIVATE NETWORKS

Inventors: Dongsoo S. Kim, Antonio Ruiz, Dhadesugoor R. Vaman, Joonbum Byun

This is a continuation in part of Serial No. 09/395,831 filed September 14, 1999.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The invention relates to protection switching for transmission systems, and more particularly to application of protection switching for virtual private networks (VPNs).

2. Art Background

Network congestion control methods address the capacity of a network as a whole to carry the offered traffic. In contrast, flow control methods address the point-to-point communication between a sender and a receiver, by adapting the data rate of the sender to the data rate at which the receiver can process the traffic. Basically, congestion control methods address the ability of a network to handle traffic, while flow control addresses the ability of the receiving devices to follow the speed of the transmitting devices.

The majority of congestion control methods have traditionally been categorized as part of traffic management. Therefore, congestion control methods used in the past have involved methods that rely on modifying or shaping the traffic at the traffic source, or at the network entrance point, in order to prevent or to handle congestion. Typical congestion control techniques include "open loop" and "closed loop" methods. The open loop methods, by definition, involve steps the network takes prior to servicing the traffic.

All open loop methods are based on pre-dimensioning the network and do not follow the dynamic changes in the traffic using the network.

Closed loop methods, on the other hand, are based on feedback received from the network. Closed loop techniques monitor the system to detect the time and location of congestion occurrence, convey the congestion notification to the parts of the system that can adjust the system operation, and ultimately, adjust the system operation. Closed loop methods are reactive in the sense that they do not act until congestion is already in place, and therefore service degradations may occur.

For the case of a fault in a transmission channel of the communication system – *e.g.*, a channel failure which results in the loss of all data being transmitted via the channel, it is known to provide a protection channel for rerouting of the data from the channel experiencing the fault. The routing of traffic from a faulty channel onto the protection channel is known as protection switching.

Virtual Private Networks (VPNs) represent a class of transmission services for which congestion control has not been effectively developed. VPNs permit implementation of a private network through utilization of the public network infrastructure. Such networks may be implemented using technologies such as Internet Protocol (IP), Frame Relay, and Asynchronous Transfer Mode (ATM).

Accordingly, the need arises for protection switching of VPNs so that data can be reliably transmitted from source to destination at all times and especially during network

failure. Additionally, the need arises for protection switching of VPNs so that network congestion can effectively be handled.

OBJECTS AND SUMMARY OF THE INVENTION

It is an object of the invention to provide a method and apparatus for protection switching of virtual private networks (VPNs) which allows data to be reliably transmitted across a VPN through the use of working and protection VPN paths and detection and switching of data between those paths.

It is yet another object of the present invention to provide for the detection of increased data traffic and errors on a working VPN path.

It is still another object of the present invention to provide for the switching of data from a working VPN path to a protection VPN path when increased data traffic and errors are detected on the working VPN path.

It is an additional object of the present invention to provide for the detection of a return-to-normal condition of a VPN path.

It is a further object of the present invention to provide for the switching of data from a protection VPN path to a working VPN path when a return-to-normal condition is detected on the working VPN path.

It is another object of the present invention to provide for data capacity management of a VPN path through the use of virtual bandwidth classes.

It is a further object of the present invention to provide for the establishment of different classes of qualities of service (QoS's).

Protection switching of a virtual private network is provided whereby working VPN paths and protection VPN paths are defined. The working VPN path is monitored for traffic congestion and failures, and in response, data is switched from the working VPN path to the protection VPN path. The working VPN path is monitored for a return to proper functioning and normal data conditions, and data is then switched back from the protection VPN path to the working VPN path. Additionally, data capacity is managed through virtual bandwidth classes, and different classes of qualities of service are provided.

BRIEF DESCRIPTION OF THE DRAWINGS

Other important objects and features of the invention will be apparent from the following Detailed Description of the Invention taken in connection with the accompanying drawings in which:

FIG. 1 is a schematic diagram showing protection switching for a virtual private network originating and terminating at the enterprise.

FIG. 2 is a schematic diagram showing protection switching for a virtual private network originating and terminating at a service provider point of presence (POP).

FIG. 3 is a block diagram showing the organization of channel capacity of the present invention.

FIG. 4 is a block diagram showing the organization of management channels.

FIG. 5 is a block diagram showing the organization of user information blocks and block overheads.

FIG. 6 is a diagram showing increased data traffic detection and handling along a VPN.

DETAILED DESCRIPTION OF THE INVENTION

The invention relates to a method and apparatus for protection switching in a virtual private network. The invention can be implemented in any VPN environment, including, but not limited to: secured Internet, encapsulated IP protocol, Layer 2 switching in ATM, and Layer 2 switching in Frame Relay.

In the parent application, a method was disclosed for detection of either congestion or link failure in an ATM network, with the method further operating to

implement a working and a protection path for links in the ATM network and to cause a switch of traffic from the working path to the protection path in case of such detection. In the case of a link failure, the method of the parent invention operates to cause all traffic on the failed link to be switched to the protection path. For the case of congestion detected on a link that exceeds a predetermined threshold, the method of the parent invention operates to cause a portion of the traffic on the working path for the link to be shifted to the protection path. The method of the parent invention also monitors failed or excessively congested working paths, and upon such a working path returning to a state of normal operation which would accommodate traffic having been switched to the protection path, operates to switch that protection path traffic back to the working path.

The present invention embodies a similar protection switching arrangement for VPN applications – *i.e.*, detection of congestion or link failure in a VPN link and, upon such detection, switching at least a portion of the traffic on the link to a protection path. An algorithm for carrying out the method of the invention may be implemented in software, firmware, or hardware, depending upon the specific implementation of protection switching, including where the VPN originates and terminates to form matched pairs that define the protection switching arrangement for the VPN domain.

The protection switching method and apparatus of the present invention embodies the following steps:

1. The definition, allocation, operation, management, and implementation of a working VPN path, over which the normal operation of the VPN is effected.

2. The definition, allocation, operation, management, and implementation of a protection VPN path, over which the protection switching operation of the VPN is effected.

3. The configuration and implementation of the working VPN path and the protection VPN path prior to the operation of either path or during the operation of the working VPN path.

4. The detection of increased data traffic in the working VPN path or failure of the working VPN path.

5. The definition, allocation, operation, management, and implementation of a VPN switching agent, whereby data from the working VPN path is switched to the protection VPN path when increased data traffic or failure is detected in the working VPN path.

6. The detection of a return to proper function of the working VPN path.

7. The definition, allocation, operation, management, and implementation of a second VPN switching agent, whereby data from the protection VPN path is switched to the working VPN path when a return to proper functioning of the working VPN path is detected.

In a further embodiment of the invention, the step of defining, allocating, operating, managing, and implementing bandwidth management arrangements in the working VPN path and the protection VPN path may also be implemented for different quality-of-service (QoS) classes.

The establishment of working and protection VPN paths may be accomplished by methods currently known in the art. In conjunction with such known methods, the present invention establishes distinct sets of VPNs that may share originating and terminating endpoints, but minimizes shared virtual or physical paths or circuits.

FIGS. 1 and **2** illustrate the method of the present invention utilized in an apparatus that works in at least two environments, namely, in the enterprise, and at a service provider's point of presence (POP). Those applications are described below.

FIG. 1 is a schematic diagram showing protection switching **10** for a virtual private network originating and terminating at the enterprise. A computer system **20** existing within an enterprise is connected to an edge router **30** for the transmission of data across a VPN. Edge router **30** establishes a VPN connection with a remote edge

router **35** by establishing a working VPN path **40** and a protection VPN path **50** between edge router **30** and remote edge router **35**. Additionally, different QoS profiles may be configured by edge router **30** by setting up additional working VPN paths **40** and protection VPN paths **50** for each QoS profile. Further, working VPN path **40** and protection VPN path **50** may be configured by edge router **30** and remote edge router **35** prior to the operation of either working VPN path **40** and protection VPN path **50**, or during the operation of working VPN path **40**.

Data is transmitted from edge router **30** to remote edge router **35** through working VPN path **40**. Once data arrives at remote edge router **35**, it is then forwarded to system **60**, the destination of the data. Significantly, in a preferred embodiment, both edge router **30** and remote edge router **35** include a monitor/detection function which operates to monitor working VPN path **40** to determine if data congestion or failure occurs in working VPN path **40**. If congestion or failure is detected, data is transferred from working VPN path **40** to protection VPN path **50**, thereby ensuring seamless data transmission. Additionally, both edge router **30** and remote edge router **35** monitor working VPN path **40** for a return-to-normal condition (i.e., a lack of congestion or failure), and upon such return-to-normal condition being detected, data is switched back from protection VPN path **50** to working VPN path **40**. Data arriving at remote edge router **35**, via either working VPN path **40** or protection VPN path **50**, is then sent to system **60**, the destination of the data.

In addition to defining working VPN path **40** and protection VPN path **50**, the invention establishes and maintains management VPN path **45** between edge router **30** and remote edge router **35**. In this arrangement, management VPN path **45** synchronizes edge router **30** and remote edge router **35**, and preferably utilizes no more than 10% of the total bandwidth of the VPN. Management VPN path **45** manages the transmission of data across working VPN path **40** and protection VPN path **50**, and allows for "hitless" data transmission. Thus, when data is transferred from working VPN path **40** to protection VPN path **50**, management VPN path **45** transfers any data lost during the switching of data from working VPN path **40** to protection VPN path **50**. Further, time stamps transferred across working VPN path **40** and protection VPN path **50** are used in combination with management VPN path **45** to achieve "hitless" data transmission.

FIG. 2 is a schematic diagram showing the protection switching **100** for a virtual private network originating and terminating at a service provider point-of-presence (POP). A computer system **120** is connected to a router **110** for transmission of data to and from the VPN. Router **110** controls the flow of data to and from computer system **120** and may be based on any of the available router technologies. Router **110** may also form part of a service provider's POP. Data that is allowed to pass from computer system **120** through router **110** is then forwarded to edge switch **130**.

Edge switch **130** establishes connection with remote edge switch **135** through working VPN path **140** and protection VPN path **150,** which provide parallel paths between the switches. A separate working-path/protection-path pair corresponding to

working VPN **140** and protection VPN path **150** may be established for each of a plurality of QoS profiles. Working VPN path **140** and protection VPN path **150** may be configured by edge switch **130** and remote edge switch **135** prior to the operation of working VPN path **140** and protection VPN path **150**, or during the operation of working VPN path **140**.

As with the embodiment of FIG. 1, this embodiment of the invention incorporates a monitor/detection function that operates to detect data congestion or failure occurring in either working VPN path **140** or protection VPN path **150**. In a preferred embodiment, that function is incorporated into edge switch **130** and remote edge switch **135**. Data arriving at edge switch **130** is transmitted through working VPN path **140** to remote edge switch **135**. Importantly, both edge switch **130** and remote edge switch **135** monitor working VPN path **140** in the same fashion as described for **FIG. 1**, above. If congestion or malfunctioning of working VPN path **140** is detected by either edge switch **130** or remote edge switch **135**, data is transferred from working VPN path **140** to protection VPN path **150**. Protection VPN path **150** is then used to transfer data between edge switch **130** and remote edge switch **135**. Edge switch **130** and remote edge switch **135** continually monitor working VPN path **140** to detect a return to normal operating condition for that path (*i.e.,* an absence of congestion or malfunction). If such a return-to-normal condition is detected, data is switched back from protection VPN path **150** to working VPN path **140**.

Data arriving at remote edge switch **135**, via either working VPN path **140** or protection VPN path **150**, is then forwarded to router **110**, which may form a part of a service provider's POP. If the data is accepted by router **110**, it is then passed to its destination, system **160**.

In addition to defining working VPN path **140** and protection VPN path **150**, the invention establishes and maintains management VPN path **145** between edge switch **130** and remote edge switch **135**. In this arrangement, management VPN path **145** synchronizes edge switch **130** and remote edge switch **135**, and preferably utilizes no more than 10% of the total bandwidth of the VPN. Management VPN path **145** manages the transmission of data across working VPN path **140** and protection VPN path **150**, and allows for "hitless" data transmission. Thus, when data is transferred from working VPN path **140** to protection VPN path **150**, management VPN path **145** transfers any data lost during the switching of data from working VPN path **140** to protection VPN path **150**. Further, time stamps transferred across working VPN path **140** and protection VPN path **150** are used in combination with management VPN path **145** to achieve "hitless" data transmission.

The protection switching arrangement of the invention enables the handling of network abnormalities, including, but not limited to, failures and congestion, in a seamless manner with respect to user applications. That protection switching arrangement treats excessive traffic congestion as a network failure, and switches data accordingly, thereby maintaining a required QoS for a given VPN.

In a preferred embodiment, a High Quality ("HQ") apparatus is implemented to carry out a detection and monitoring function, as to failures and excessive congestion, for the protection switching arrangement of the invention. That HQ apparatus may be operated independently of the router or switch operating at either end of a given working path and its associated protection path, or it may be incorporated into the router/switch with which it is associated. Operation of an exemplary HQ apparatus, based on an exchange of header, or overhead, data associated with data blocks being transmitted, is hereafter described. Other arrangements for implementation of the disclosed detection/monitoring function will, however, be apparent to those skilled in the art. All such implementations are intended to be within the scope of the invention disclosed and claimed herein.

For the preferred embodiment, the detection of network congestion and link failure (and corresponding protection switching based thereon) is enabled through the use of block overheads ("BLOHs") for the data being transmitted. Blocks can be cells for ATM transport or packets for IP or any native mode transport information in each VPN path or channel. Each BLOH consists of the following fields, each of which can be expanded for future enhancements:

Block 1: High priority block (loop-back block for congestion prevention)

Block 2: Low priority block (loop-back block for congestion prevention)

Blocks 3-12: Loop-back blocks (for loss detection)

Block 13: Current initial block ID with time stamp for block frame, sent on the working VPN path

Block 14: Current final block ID with time stamp for block frame, sent on the working VPN path

Block 15: Next initial block ID for the working VPN path

Block 16: Next final block ID for the working VPN path

(next 16 blocks reserved for future usage.)

The above block layout is common to all BLOHs for signals utilizing VPNs operate according to the protection switching methodology of the invention. Hitless network operation is disclosed in the U.S. Patent Application Serial No. 09/249,001, filed February 12, 1999, now U.S. Patent No. _____, the entire disclosure of which is expressly incorporated herein by reference.

An exemplary channel arrangement for the VPN protection-switching methodology of the invention is illustrated in **FIG 3.** Both the general operation of that protection switching methodology and the particular role of the BLOHs in that operation are usefully described with respect to that figure. The protection switching methodology **70** of the invention begins with operation of HQ apparatus **72**, which establishes a first VPN **74** and a second VPN **76**. It is to be understood that additional VPNs may be established by HQ apparatus **72**. First VPN **74** and second VPN **76**, including any additional VPNs, are connected to edge router **78**. Edge router **78** then connects the VPNs across working path **80** and protection path **86** utilizing first channel **82** and second

channel **84**. Additional channels may be included in the present invention. Once VPNs are connected through working path **80** and protection path **86** utilizing either first channel **82** or second channel **84**, the VPNs are connected to remote edge router **88**, where they ultimately can be connected to the destination network or machine.

The management channel of the present invention can be used to monitor and detect problems on the working path and to switch data from the working path to the protection path in response to a failure of or congestion in the working path. The management channel comprises information that is transmitted through the working path of the VPN in conjunction with time stamps and other measurement parameters. No synchronization is required between the end nodes connected by the working and protection paths. Further, information transmitted in the management channel can be analyzed by algorithms that detect failures and the onset of congestion in the working path. Generally, the amount of bandwidth used by the management channel is substantially lower than the bandwidth used by the working path.

VPNs utilizing channels **82** and **84** of **FIG 3** may be organized in the following fashion:

VPNi1, VPNi2, …, VPN ii may be used for user information paths;

VPNij may be used as a spare or for a protection path; and

VPNin may be used as a management path for HQ device or edge routers

HQ device **72** sets up working path **80**. VPNi1 for a user application is sent along working path **80** using channel **82**. Simultaneously, VPNk1, also used for the same user application, is sent along protection path **86** using channel **84**. HQ device **72** continually tracks the availability of spare VPNij and management VPNin. Protection switching between working path **80** and protection path **86** occurs when working path **80** fails. In such an event, HQ apparatus **72** switches over to protection path **86**. Information being sent on working path **80** at the time of a failure is sent to protection path **86**. Time stamps embedded in the BLOHs allow for seamless recovery of data when a switch between working path **80** and protection path **86** occurs. For hitless operation, the current block is copied at the sending side and is resent on the management channel of the protection path to assure that there is no loss of information. Additionally, the current block may also be copied to the protection path to ensure data integrity.

Organization of management channels is depicted in **FIG. 4.** VPN1n and VPN2n are the management channels for operation of the network. Block overheads ("BLOH") of VPN11 through VNP1n-1 are transmitted on a first management channel **90**, while BLOHs of VPN21 through VPN2n-1 are transmitted on a second management channel **100**.

FIG. 5 is a diagram showing an arrangement of BLOHs for the method of the invention. User information and block overheads may be transmitted across either a working path or a protection path according to grouping **170**, whereby block overheads are transmitted in sequence with one or more user blocks. Block overheads assigned to

different user blocks are also transmitted on the management channel according to grouping **180**. The block overheads of grouping **180** may originate from either the working path or the protection path.

Failure of the working path may be detected by the monitoring of varying BLOHs by the HQ device. Blocks 3-12 of each BLOH consist of a loop-back block that is sent by the sending HQ device and received by a receiving HQ device on each user channel. The receiving HQ device receives the blocks and sends them back to the sending HQ device on a reverse or management channel. The HQ device sets up a threshold that indicates whether a loss of signal has occurred. For an illustrative embodiment of the invention, the threshold is set at 70% of the blocks, or 7 blocks. If the number of blocks returned is less than or equal to the threshold, a failure of the working path is detected. Alternately, failure may be detected by the receiving HQ device by comparing the blocks it receives with the corresponding BLOHs transmitted via the management path.

In the event that a receiving HQ device determines that the threshold has been met and a failure of the working path has occurred, the HQ device waits for the sending HQ device to switch to the protection path. On the other hand, if the sending HQ device detects a failure of the working path using the threshold comparison, it re-sends the lost information between two BLOHs which are time-stamped to ensure that there is no loss of information. When the working path is later restored, both the sending and receiving HQ devices will revert to the working path.

The protection switching scheme and apparatus of the present invention also allows for the detection and handling of network congestion. Blocks 1 and 2 of the BLOH are used to detect the onset of congestion. Block 1 is a high priority block and Block 2 is a low priority block. These blocks are sent back from a receiving HQ device to a sending HQ device. Therefore, the sending HQ device can compute the round trip-trip delay of the high priority block as well as that of the low-priority block. The relative delay difference (Delta) is calculated by subtracting the round-trip delay of Block 2 from the round-trip delay of Block 1. When traffic congestion occurs in the network, then Delta increases as the network processes the low-priority block more slowly.

FIG. 6 is a diagram showing the detection and handling of congestion using the aforesaid delta values in a hysterisis function. As shown in the figure, three delay thresholds are established: Delta 1, Delta 2, and Delta C. The highest threshold, Delta C, is established at the point of maximum acceptable network congestion. The lowest threshold, Delta 1, is established at the upper limit for "normal" operation of the channel – *i.e.,* before any congestion occurs. The intermediate threshold, Delta 2, is set at a point below Delta C at which a sufficient degree of congestion occurs to merit off-loading of traffic to another channel and to avoid further congestion. In a preferred embodiment, the Delta 2 threshold is maintained at less than 0.8 of Delta C. The delay differential between Delta 1 and Delta 2 is a buffer zone in which the channel may operate without off-loading traffic.

Thus, when Delta < Delta 1, the system is operating in normal mode and the working path is used to send all of the user information blocks. When Delta > Delta 2, the channel has reached an unacceptable level of congestion. In that circumstance, the data is partially split for sending a portion via the protection path along with the balance being sent via the working path. Once in the congestion area, *i.e.*, Delta > Delta C, the system waits until Delta < Delta 1 to switch back to normal mode and to re-route traffic to the working channel.

The system does not go into congestion mode unless the overall capacity is excessively over-used. This situation indicates that the capacity is not dimensioned properly for network operation. Further, the failures handled by the present invention include, but are not limited to: link failures, system failures, hardware failures, software failures, power failures, firmware failures, security failures (*i.e.*, resulting from a violation of VPN policies, firewall policies, or repeated attempted accesses from an unauthorized user or system), encryption violation (*i.e.*, the failure of a secured domain requiring a new protection path), and loss of signal in wireless systems.

Having thus described the invention in detail, it is to be understood that the foregoing description is not intended to limit the spirit and scope thereof. What is desired to be protected by Letters Patent is set for in the appended claims.